Assurance Cases

Description

Introduces the concepts and benefits of creating and maintaining assurance cases for security. A security assurance case uses a structured set of arguments and a corresponding body of evidence to demonstrate that a system satisfies specific claims with respect to its security properties.

Overview Article

Name	Version Creation Time	Abstract
Assurance Cases Overview	11/14/08 3:51:00 PM	Our objective for the Assurance Cases (AC) content area of the Build Security In (BSI) Web site is to raise awareness about emerging methods and tools for assuring security properties of systems. In this content area, we introduce the concepts and benefits of developing and maintaining assurance cases for security. In particular, we describe the benefits of integrating assurance cases for security into the software development life cycle (SDLC) by "building assurance in" from the outset.

Most Recently Updated Articles [Ordered by Last Modified Date]

Name	Version Creation Time	Abstract
Improving Software Assurance	4/7/10 12:48:15 PM	Software assurance objectives include reducing the likelihood of vulnerabilities such as those on a Top 25 Common Weakness Enumeration[1] (CWE) list and increasing confidence that the system behaves as expected. Practitioners should understand where to look, what to look for, and how to demonstrate improvement. For practitioners who want to delve deeper into software assurance, the BSI website provides a wealth of information to aid in tying security into all development activities. For example, the BSI website[2] includes a number of papers[3] that were presented at the

		Making the Business Case for Software Assurance Workshop[4] in September 2008. Today, more than 25 large-scale software security initiatives are underway in organizations as diverse as multi-national banks, independent software vendors, the U.S. Air Force, and embedded systems manufacturers. The Software Assurance Forum for Excellence in Code (SAFECode), an industry-leading non-profit organization that focuses on the advancement of effective software assurance methods, published a report on secure software development [Simpson 2008]. In 2009, the first version of The Building Security In Maturity Model (BSIMM) was published [McGraw 2009]. BSIMM was created from a survey of nine organizations with active software security initiatives the authors considered to be the most advanced. The nine organizations were drawn from three verticals: four financial services firms, three independent software vendors, and two technology firms. Those companies among the nine who agreed to be identified include Adobe, The Depository Trust & Clearing Corporation (DTCC), EMC, Google, Microsoft, QUALCOMM, and Wells Fargo.
Evidence of Assurance: Laying the Foundation for a Credible Security Case	11/14/08 3:53:58 PM	A security case bears considerable resemblance to a legal case, and demonstrates that security claims about a given system are valid. Persuasive argumentation plays a major role, but the credibility of the arguments and of the security case itself ultimately rests on a foundation of evidence. This article describes and gives examples of several of the *kinds* of evidence that can contribute to a security case. Our main focus is on how to understand, gather, and generate the kinds of evidence that

		can build a strong foundation for a credible security case.
Arguing Security - Creating Security Assurance Cases	11/14/08 3:52:06 PM	An assurance case is a body of evidence organized into an argument demonstrating that some claim about a system holds, i.e., is assured. An assurance case is needed when it is important to show that a system exhibits some complex property such as safety, security, or reliability. In this article, our objective is to explain an approach to documenting an assurance case for system security, i.e., a *security* assurance case or, more succinctly, a *security case*.
Assurance Cases Overview	11/14/08 3:51:00 PM	Our objective for the Assurance Cases (AC) content area of the Build Security In (BSI) Web site is to raise awareness about emerging methods and tools for assuring security properties of systems. In this content area, we introduce the concepts and benefits of developing and maintaining assurance cases for security. In particular, we describe the benefits of integrating assurance cases for security into the software development life cycle (SDLC) by "building assurance in" from the outset.

All Articles [Ordered by Recommended Reading Order]

Name	Version Creation Time	Abstract
Assurance Cases Overview	11/14/08 3:51:00 PM	Our objective for the Assurance Cases (AC) content area of the Build Security In (BSI) Web site is to raise awareness about emerging methods and tools for assuring security properties of systems. In this content area, we introduce the concepts and benefits of developing and maintaining assurance cases for security. In particular, we describe the benefits of integrating assurance cases for security into the software development life cycle (SDLC) by "building assurance in" from the outset.

Arguing Security - Creating Security Assurance Cases	11/14/08 3:52:06 PM	An assurance case is a body of evidence organized into an argument demonstrating that some claim about a system holds, i.e., is assured. An assurance case is needed when it is important to show that a system exhibits some complex property such as safety, security, or reliability. In this article, our objective is to explain an approach to documenting an assurance case for system security, i.e., a *security* assurance case or, more succinctly, a *security case*.
Evidence of Assurance: Laying the Foundation for a Credible Security Case	11/14/08 3:53:58 PM	A security case bears considerable resemblance to a legal case, and demonstrates that security claims about a given system are valid. Persuasive argumentation plays a major role, but the credibility of the arguments and of the security case itself ultimately rests on a foundation of evidence. This article describes and gives examples of several of the *kinds* of evidence that can contribute to a security case. Our main focus is on how to understand, gather, and generate the kinds of evidence that can build a strong foundation for a credible security case.
Improving Software Assurance	4/7/10 12:48:15 PM	Software assurance objectives include reducing the likelihood of vulnerabilities such as those on a Top 25 Common Weakness Enumeration[5] (CWE) list and increasing confidence that the system behaves as expected. Practitioners should understand where to look, what to look for, and how to demonstrate improvement. For practitioners who want to delve deeper into software assurance, the BSI website provides a wealth of information to aid in tying security into all development activities. For example, the BSI website[6] includes a number of papers[7] that were presented at the Making the Business Case for

		Software Assurance Workshop[8] in September 2008. Today, more than 25 large-scale software security initiatives are underway in organizations as diverse as multi-national banks, independent software vendors, the U.S. Air Force, and embedded systems manufacturers. The Software Assurance Forum for Excellence in Code (SAFECode), an industry-leading non-profit organization that focuses on the advancement of effective software assurance methods, published a report on secure software development [Simpson 2008]. In 2009, the first version of The Building Security In Maturity Model (BSIMM) was published [McGraw 2009]. BSIMM was created from a survey of nine organizations with active software security initiatives the authors considered to be the most advanced. The nine organizations were drawn from three verticals: four financial services firms, three independent software vendors, and two technology firms. Those companies among the nine who agreed to be identified include Adobe, The Depository Trust & Clearing Corporation (DTCC), EMC, Google, Microsoft, QUALCOMM, and Wells Fargo.